UNITED STATES PATENT AND TRADEMARK OFFICE

59

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/483,127	01/14/2000	Alan Dowd	105.176US1	7964

21186 7590 04/18/2005

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. BOX 2938
MINNEAPOLIS, MN 55402

EXAMINER	
CRAIG, DWIN M	
ART UNIT	**PAPER NUMBER**
2123	

DATE MAILED: 04/18/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.	**Applicant(s)**	
09/483,127	DOWD ET AL.	
Examiner	**Art Unit**	
Dwin M Craig	2123	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 1-8-2005 .

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-42 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-42 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)□ The proposed drawing correction filed on _____ is: a)□ approved b)□ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)□ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____ .

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) □ The translation of the foreign language provisional application has been received.

15)□ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .
4) □ Interview Summary (PTO-413) Paper No(s). _____ .
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: .

DETAILED ACTION

1. In view of the Appeal Brief filed on 1-8-2005, PROSECUTION IS HEREBY REOPENED. A new grounds of rejection to the Appeal Brief set forth below.

To avoid abandonment of the application, appellant must exercise one of the following two options:

(1) file a reply under 37 CFR 1.111 (if this Office action is non-final) or a reply under 37 CFR 1.113 (if this Office action is final); or,

(2) request reinstatement of the appeal.

If reinstatement of the appeal is requested, such request must be accompanied by a supplemental appeal brief, but no new amendments, affidavits (37 CFR 1.130, 1.131 or 1.132) or other evidence are permitted. See 37 CFR 1.193(b)(2).

Response to Arguments

2. Applicant's arguments filed on 1-8-2005 have been fully considered. The Examiner's response is as follows:

2.1 On page 13 of Applicant's Appeal Brief Applicant argued,

> *Samfat describes a mobile network simulator used to test applications, specifically a generic intrusion detection architecture...*
>
> *The Network simulation described in Samfat is limited to a narrow field of mobile networks. In contrast, Applicants describe a network simulator that simulates enterprise networks, wide area networks, local area networks and the like as well as components of networks such as servers, workstations, routers and firewalls (p.5 lines 205).*

The claims were read in light of the specification; *however,* the limitations argued are not present in the current claim language. The Examiner respectfully notes that the *network* being claimed by the Applicant does not exclude a wireless *network.*

Further, the Examiner notes the following in regards to claim interpretation during Patent prosecution, MPEP § 2111, under the heading "Claims Must Be Given Their Broadest Reasonable Interpretation," states, in reference to *In re Prater,* 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-51 (CCPA 1969):

"The court explained that "reading a claim in light of the specification, [ʻ] to thereby interpret limitations explicitly recited in the claim, is a quite different thing from ʻreading limitations of the specification into a claim,ʼ to thereby narrow the scope of the claim by implicitly adding disclosed [sic, disclosed] limitations which have no express basis in the claim."

2.2 On page 14 of Applicant's Appeal Brief Applicant argued,

Samfat teaches that by using a simulator to develop a Network Management System problems unique to a mobile network are avoided. Specifically, problems involving the unavailability of existing networks during the software development phase and the provision of a wide range of traffic generators over a wide geographic area are avoided. Samfat also teaches that simulators allow repeatability over excessive runs and the value of a static network configuration for repeatable software testing.

In contrast, Appellants teach a system for assessing network vulnerabilities in an objective network, and not for debugging software. This is significant, because while in some cases similar conditions may be repeated, Appellants teach that by allowing the system administrator or user to modify configuration data, information can be gleamed as to what effect adding or removing a device might have on the objective network before physically modifying the network (p. 6, lines 12-17). Because the simulators are significantly different themselves and also because the purpose and use of the simulators are distinct, it would not have been obvious to combine the references. Appellants respectfully request that this rejection be withdrawn.

The claims were read in light of the specification; *however,* the limitations argued are not present in the current claim language. The Examiner respectfully notes that the limitations of *having the administrator or user modify configuration data*, is not disclosed in the current claim language.

Further, the Examiner notes the following in regards to claim interpretation during Patent prosecution, MPEP § 2111, under the heading "Claims Must Be Given Their Broadest Reasonable Interpretation," states, in reference to *In re Prater,* 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-51 (CCPA 1969):

"The court explained that "reading a claim in light of the specification, [ʻ] to thereby interpret limitations explicitly recited in the claim, is a quite different thing from ʻreading limitations of the specification into a claim,ʼ to thereby narrow the scope of the claim by implicitly adding disclosed [sic, disclosed] limitations which have no express basis in the claim."

2.3 On page 14 of Applicant's Appeal Brief Applicant argued,

> *Appellants teach that the simulator can be used both for specific attack scenarios or general attack scenarios (p. 6, lines 15-17). In addition, user defined security checks are disclosed by Applicants (p.7, lines 7-9). Therefore, no combination of the references discloses the more rigorous simulation and analysis described by Appelants.*

The claims were read in light of the specification; however, the limitations argued are not present in the current claim language. The Examiner respectfully notes that nowhere in the current claim language is the distinction made between *general attack scenarios vs. specific attack scenarios.*

Further, the Examiner notes the following in regards to claim interpretation during Patent prosecution, MPEP § 2111, under the heading "Claims Must Be Given Their Broadest Reasonable Interpretation," states, in reference to *In re Prater,* 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-51 (CCPA 1969):

"The court explained that "reading a claim in light of the specification, [ʻ] to thereby interpret limitations explicitly recited in the claim, is a quite different thing from ʻreading limitations of

the specification into a claim,' to thereby narrow the scope of the claim by implicitly adding disclosed [sic, disclosed] limitations which have no express basis in the claim."

2.4 On page 15 of Applicant's Appeal Brief Applicant argued,

> *Thus, while Gleichauf describes a database of network vulnerabilities organized in a hierarchical structure where each entry contains an operating system represented by the entry, a service to which it applies and a potential vulnerability, the reference does not teach that these vulnerabilities include "defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability," (Claims 1 and 18).*

It would be obvious, to provide methods of protecting a computer system on a network when using vulnerability assessment tool. It is known in the network security art that the whole purpose of performing network vulnerability testing is to know where to implement adjustments to the current network systems to compensate for any newly discovered vulnerabilities, *Gleichauf et al. (U.S. Pat. No. 6,282,546)* discloses, *(Col. 4 lines 38-46, "This intrusion data then augments the vulnerability data already stored within the multi-dimensional database **12**. Subsequently, user interface **14** can operate, passively and <u>actively</u>, to provide visibility and <u>response</u> to this inserted data... Actively, user interface **14** could monitor certain cells and category's of data and react to insertions by notifying a network administrator (e.g., by e-mail, pager, call, alarm, etc.).")*

The *active* form of the user interface performs is the functional equivalent of *defense conditions*. Note in **Figure 3A**, of the *Gleichauf et al. (546')* reference, items **32** where the ports and service(s) being attacked are being identified. An artisan of ordinary *network security* skill would know that these are the ports i.e. *"resource"* and services i.e. *"state"* that need to be *modified* and/or *shut down* to close the vulnerability. Thus, the *Gleichauf et al. (546')* reference is disclosing the functional equivalent of the methods to, *close the vulnerability, and resource and state conditions needed to exercise the vulnerability," (Claims 1 and 18).*

2.5 On page(s) 15 & 16 of Applicant's Appeal Brief Applicant argued,

> *In contrast, Appellants teach a game with a modeled network that behaves accurately enough to train system administrators and other personnel on how to build and protect secure networks (p.20, lines 5-7).*

The claims were read in light of the specification; however, the limitations argued are not present in the current claim language. The Examiner respectfully notes that nowhere in the current claim language are the limitations expressly claiming the use of the *game* to *train system administrators on how to build and protect secure networks.*

Further, the Examiner notes the following in regards to claim interpretation during Patent prosecution, MPEP § 2111, under the heading "Claims Must Be Given Their Broadest Reasonable Interpretation," states, in reference to *In re Prater,* 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-51 (CCPA 1969):

> *"The court explained that "reading a claim in light of the specification, ['] to thereby interpret limitations explicitly recited in the claim, is a quite different thing from 'reading limitations of the specification into a claim,' to thereby narrow the scope of the claim by implicitly adding disclosed [sic, disclosed] limitations which have no express basis in the claim."*

2.6 On page 16 of Applicant's Appeal Brief Applicant argued,

> *While Jackson does teach that playing an Illuminati style card game is something people like to do, the reference does not show that playing a computer game involving attacking or defending an accurate simulation of a realistic network is something people like to do.*

Taking any game and transforming it into a computer game is obvious, multiplayer network based games, where there is an a attacker and a defender were well known in the art at the time the Applicant's invention was made. An example of computer games with attackers and defenders is the game *"Star Craft®"* by Blizzard entertainment. Further, *Jackson* clearly discloses that there was a *large* demand for this game product *(...on the back cover of the game is disclosed, "In 1990, Steve Jackson Game was raided by the U. S. Secret Service when a "hacker hunt" went out of control. Ever since then, fans have been asking, "When are you going to make a game out of it?" Okay. We give up. Here it is.).* It is clear from the preceding quote from *Jackson* that there was a *demand* and *interest* for people to play a game involving *hacking* into a computer system.

2.7 On page(s) 16 & 17 of Applicant's Appeal Brief Applicant argued,

> *The Examiner stated that Bergmann discloses determining network components that are involved in a specific attack scenario... While Bergmann has relevance in network in network security applications, the system does not serve the purpose that the Appellant's mission objective module does in determining components involved in an attack scenario. Appellants teach knowing which components are likely to be involved in an attack scenario before and after the simulation is run in order to assess the security of the network. In contrast, Bergmann teaches a defensive method and system for protecting the integrity and efficiency of a network against an attack in progress.*

Note in **Figure 3A**, of the *Gleichauf et al. (546')* reference, items **32** where the ports and service(s) being attacked are being identified. The Examiner notes that *Gleichauf et al. (546')* discloses determining network components that are involved in a specific attack scenario, or *critical resource information* (the cells in the *Gleichauf et al. (546')* reference could be *critical resources),* **(Figure 2 item 24 "Identify Cell(s) Associated with Event").**

Further and in regards to Applicant's arguments, *Bergmann* was relied upon to teach only that *specific* network resources could be identified during an attack simulation.

As regards Applicant's argument that *Bergmann* does not disclose, *knowing which components are likely to be involved in an attack scenario before and after the simulation is run in order to assess the security of the network.*

The claims were read in light of the specification; however, the limitations argued are not present in the current claim language. The Examiner respectfully notes that nowhere in the current claim language are the limitations expressly claiming, *knowing which components are likely to be involved in an attack scenario before and after the simulation is run in order to assess the security of the network.*

Further, the Examiner notes the following in regards to claim interpretation during Patent prosecution, MPEP § 2111, under the heading "Claims Must Be Given Their Broadest Reasonable Interpretation," states, in reference to In re Prater, 415 F.2d 1393, 1404-05, 162 USPQ 541, 550-51 (CCPA 1969):

> *"The court explained that "reading a claim in light of the specification, ['] to thereby interpret limitations explicitly recited in the claim, is a quite different thing from 'reading limitations of the specification into a claim,' to thereby narrow the scope of the claim by implicitly adding disclosed [sic, disclosed] limitations which have no express basis in the claim."*

2.8 On page 17 of Applicant's Appeal Brief is argued,

> *Regardless of whether Smith Jr. teaches mission objectives, or missions and objectives, they are of a distinctly different character than the mission objectives module Applicants disclose. Missions and objectives in the context of Smith Jr. relate to generic problem solving goals. In contrast, Appellants teach mission objectives of a different kind, used to determine which components are involved in a specific network simulation and including critical resource information.*

Gleichauf et al. 546' discloses, *determin(ing) which components are involved in a specific network simulation…including critical resource information* see section 2.7 above. In regards to *Smith Jr.* teaching *mission objectives,* the meaning of words used in a claim are not construed in a "lexicographic vacuum", but in the context of the specification and drawings." *Toro Co. v. White Consolidated Industries Inc., 199 F.3d 1295, 1301, 53 USPQ2d 1065, 1069 (Fed. Cir. 1999).* Only in such a forbidden "lexicographic vacuum" could "mission objectives" mean something different from what the Applicant's specification has defined as "mission objectives".

When given the broadest reasonable interpretation "consistent with the specification," as it must be, *In re Hyatt 21 1 F.3d 1367, 1372, 54 USPQ2d 1664, 1667 (Fed. Cir. 2000) (Emphasis added),* it is manifestly unreasonable to equate the phrase disclosed and described in the Applicant's specification to have any other meaning than that which is disclosed in that very same specification.

The Examiner notes that on page 9 of Applicant's specification is disclosed the following, *"The mission objectives module 207 which is coupled to the simulator 201 includes critical resource information such as goals, expectations and constraints for simulating the network. "* The Examiner can find no other embodiment that is contrary to this definition. The definition includes *goals,* which by Applicant's own argument, the *Smith Jr.* reference teaches, the definition also includes, expectations and constraints, its is obvious that the expectation is that the network will be simulated, *Gleichauf et al. 546'* teaches, *determin(ing) which components are involved in a specific network simulation...including critical resource information* which then covers the *constraints* of the simulation. The combination of *Gleichauf et al 546'* and *Smith Jr.* disclose and make obvious, the definition of *mission objectives* as defined in Applicant's specification.

2.9 On page 17 of Applicant's Appeal Brief is argued,

> *The Examiner stated that Jackson discloses mission objectives. Jackson describes mission objectives in the context of gaining access to a given number of systems in order for a player to win a game. In contrast, Appellants teach using mission objectives that include critical resource information in order to determine components involved in a specific attack scenario. Also, as discussed above, there is no motivation to combine the references, because Jackson does not teach an accurate model of a network, but rather a stylized card game using hacker terminology.*

Jackson discloses a game for simulation of attacking computer systems on a network. Applicant is claiming, *a computer game comprising network configuration data* (***Jackson discloses network configuration data pages 4 & 5*** *"Direct Connections," Hub Connections" "System types"*) describe network configuration data. *A simulator coupled to the network configuration module,* is disclosed in *Jackson,* because it is a *"game"* and the game is simulating a network. *Jackson* has to simulate a network to function, so by definition, the game Hacker is a simulation of a network. The Applicant has argued that *Jackson* does not teach an *accurate* model of a network, however, Applicant's claim language does not contain a limitation that an *accurate* model of the network is required for the simulation. Applicant has claimed that the *network configuration module* contains *network configuration data*, however the *accuracy* of this data is neither claimed nor disclosed in the specification. Applicant has argued that this data comes from an *actual* network and *for example* in dependent claim 4 the Applicant claimed that the data comes from a *network configuration discovery tool.* The Examiner notes that the *Gleichauf et al. 656'* reference discloses a *network discovery tool*, which would then provide data for an *accurate* model of a simulated network. As argued in section 2.8 above the Examiner argued that the *mission objectives module* is disclosed in the combination of the *Smith* and *Gleichauf et al. 546'* references.

Further, the definition of what is a *game* is subjective, specifically as regards if the system claimed is a tool or a game. If an artisan has a tool and is being paid to use that tool then the game is really a tool and not a game. If the artisan is using the tool for fun and enjoyment, then the tool is really a game or a toy. It is unclear if there is an embodiment in the Applicant's specification that specifically discloses a *game*.

In conclusion the Examiner notes that the *Gleichauf et al. '546* reference discloses **Col. 2 lines 32-35** which teaches *any correlation to known aspects of the network environment,* as disclosed form the *multidimensional* database. *Known aspects* of a *network environment* is the functional equivalent of a *known constraint* of the network environment, which was disclosed in Applicant's specification as the part of the definition of the *mission objectives module.*

2.10 On page 17 of Applicant's Appeal Brief is argued,

> *While Gleichauf 2 does disclose vulnerability tables and network configuration tables, the reference does not disclose mission objective tables. Appellants teach that mission objective tables are a valuable tool in determining attack scenarios and also evaluating network security.*

The Examiner notes that the definition of *mission objective tables* that Applicant is arguing in this response is not reflected in the current claim language or is not the same as is disclosed in Applicant's. Please see section 2.8 above.

2.11 The Examiner respectfully traverses Applicant's arguments and upholds the earlier rejections of claims 1-42. An updated search has revealed new art.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Independent **Claims 1 and 18** and dependent **Claims 2, 4, 5, 8 and 19** are rejected under 35 U.S.C 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362** and in further view of "**A GSM Simulation Platform for Intrusion Detection**" by **Didier Samfat, Veronique Devernay and Christian Bonnet** *hereafter referred to as the Samfate et al. reference.*

3.1 As regards independent **Claims 1 and 18** the *Gleichauf et al.* reference discloses a security modeling system **(Col. 2 Lines 47-50, Col. 4 Lines 20-43)**, a network configuration module having network configuration data **(Col. 4 Lines 9-19 Figure 2, Col. 5 Lines 14-26)**, a computer implemented method of analyzing networks based on the network configuration data where the software includes a network vulnerabilities database where the network vulnerabilities database includes, a plurality of known network vulnerabilities where each network vulnerability includes a service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability, **(Figures 1-5, Figure 5 ITEMS 26 and 126, Col. 6 Lines 21-25, Col. 7 Lines 5-54).**

However, the *Gleichauf et al.* reference does not expressly disclose a network simulation for analyzing attacks against a network.

The *Ptacek et al.* reference discloses a network simulation for analyzing attacks against a network **(Col. 3 Lines 24-43).**

It would have been obvious, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Ptacek et al.* reference because, *(motivation to combine)* the *Ptacek et al.* reference discloses a method of simulating attacks on a network and provides a means to test the vulnerability of an proposed network configuration against different types of attacks without exposing that network to an actual attack.

However, the *Gleichauf et al.* reference does not expressly disclose a network simulation.

The *Samfate et al.* reference discloses a network simulator **(page 766).**

It would have been obvious, to one of ordinary skill in the art, at the time the invention was made, to have combined the *Network vulnerability database* of the *Gleichauf et al.* reference with the network simulator of the *Samfate et al.* reference because, by being able to exactly repeat the manner in which the network behaves as the attack takes place, software counter measures can be tested, and then retested in an environment where the same conditions can be repeated when debugging the counter measure software **(*Samfate et al. page 766*).**

3.2 As regards dependent **Claim 2** the *Gleichauf et al.* reference discloses a database, including network vulnerability and exploitation data and attack data **(Figure 2 ITEM 80, Figure 3A ITEM 98, Figure 3B, 4 and 5, Col. 4 Lines 9-19, Col. 8 Lines 13-25).**

3.3 As regards dependent **Claims 4 and 19** the *Gleichauf et al.* reference discloses a network configuration discovery tool **(Figure 3A, ITEMS 90 and 92, Col. 2 Lines 6-15).**

3.4 As regards dependent **Claim 5** the *Gleichauf et al.* reference does not expressly disclose a Graphical User Interface.

The *Ptacek et al.* reference discloses a Graphical User Interface **(Figure 2A, ITEM 260, Col. 4 Lines 59-67, Col. 5 Lines 1-9).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Ptacek et al.* reference because, *(motivation to combine)* a Graphical User Interface provides an easy to use method of user interaction with a computer program that does not require the user to memorize large amounts of command line interface commands to perform useful tasks.

3.5 As regards dependent **Claim 8** the *Gleichauf et al.* reference discloses a portable modeling system **(Figure 1 ITEMS 20, 22, 24 and 26).**

4. Dependent **Claims 3 and 6** are rejected under 35 U.S.C 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362** and in further view of "**A GSM Simulation Platform for Intrusion Detection"** by **Didier Samfat, Veronique Devernay and Christian Bonnet** *hereafter referred to as the Samfate et al. reference* and in further view of **Gleichauf et al. U.S. Patent 6,282,546** *hereafter referred to as the G2 reference.*

4.1 As regards independent **Claim 1** see paragraph 3.1 above.

4.2 As regards dependent **Claim 2** see paragraph 3.2 above.

4.3 As regards dependent **Claim 3** the *Gleichauf et al.* reference does not expressly disclose database tables.

The *G2* reference discloses database tables **(Figure 3B and 3C).**

It would have been obvious to combine the *Gleichauf et al.* reference with the *G2* reference because, the *Gleichauf et al.* reference specifically points the reader to the *G2* reference in **(Col. 8 Lines 12-25)** when discussing another embodiment of the invention disclosed in the *Gleichauf et al.* reference.

4.4 As regards dependent **Claim 6** the *Gleichauf et al.* reference does not expressly disclose receiving the network vulnerability, attack and exploitation data.

The *G2* reference discloses receiving updated network vulnerability, attack and exploitation data **(Figure 1 ITEMS 18 and 16).**

It would have been obvious to combine the *Gleichauf et al.* reference with the *G2* reference because, the *Gleichauf et al.* reference specifically points the reader to the *G2* reference in **(Col. 8 Lines 12-25)** when discussing another embodiment of the invention disclosed in the *Gleichauf et al.* reference.

5. Dependent **Claim 7** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362** and in further view of "**A GSM Simulation Platform for Intrusion Detection**" by **Didier Samfat, Veronique Devernay and Christian Bonnet** *hereafter referred to as the Samfate et al. reference* and in further view of **Sparks, II U.S. Patent 6,352,479.**

5.1 As regards independent **Claim 1** see paragraph 3.1 above.

5.2 As regards dependent **Claim 7** the *Gleichauf et al.* reference does not expressly disclose a simulator with an attacker and a defender user interface.

The *Sparks II* reference discloses an attacker and a defender user interface **(Figure 3).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Sparks II* reference because, *(motivation to combine)* by supporting multiple players using a network and graphical user interfaces, complex and real-time interaction between an attacker and a defender can be achieved over great distances using a network, like the internet, where two people do not have to be in the same geographic location to play against each other in a simulation or a game **(*Sparks II, Col. 1 Lines 50-65*).**

6. Independent **Claim 9** is being rejected under 35 U.S.C. 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362** and in further view of "**A GSM Simulation Platform for Intrusion Detection**" by **Didier Samfat, Veronique Devernay and Christian Bonnet** *hereafter referred to as the Samfate et al. reference* and in further view of **Sparks, II U.S. Patent 6,352,479.**

6.1 As regards independent **Claim 9** the *Gleichauf et al.* reference discloses a network configuration module **(Col. 4 Lines 9-19 Figure 2, Col. 5 Lines 14-26),** a computer implemented method of analyzing networks based on the network configuration data where the software includes a network vulnerabilities database where the network vulnerabilities database includes, a plurality of known network vulnerabilities where each network vulnerability includes a service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability, **(Figures 1-5, Figure 5 ITEMS 26 and 126, Col. 6 Lines 21-25, Col. 7 Lines 5-54).**

However, the *Gleichauf et al.* reference does not expressly disclose a network simulation or a computer game.

The *Ptacek et al.* reference discloses a network simulation for analyzing attacks against a network **(Col. 3 Lines 24-43).**

It would have been obvious, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Ptacek et al.* reference because, *(motivation to combine)* the *Ptacek et al.* reference discloses a method of simulating attacks on a network and provides a means to test the vulnerability of an proposed network configuration against different types of attacks without exposing that network to an actual attack.

The *Sparks II* reference discloses a computer game **(Figures 1-12).**

It would have been obvious, to one of ordinary skill in the art, to have combined the *Gleichauf et al.* reference with the *Sparks II* reference because, *(motivation to combine)* by playing a game using the game server disclosed in the *Sparks II* reference the player is able to be handicapped in a manner to determine the current level of skill and this is useful in determining if that particular individual is ready for operating at a particular skill level. In the manner described a computer security expert could determine if a particular person is qualified to receive a certification for a particular job protecting a computer network **(Sparks II, Figure 12)**.

7. Independent **Claim 10** and dependent **Claims 11, 13, 14 and 16** are being rejected under 35 U.S.C. 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362** and in further view of "**A GSM Simulation Platform for Intrusion Detection**" by **Didier Samfat, Veronique Devernay and Christian Bonnet**

hereafter referred to as the Samfate et al. reference and in further view of **Bergman et al. U.S. Patent 6,422,694** and in further view of **Smith, Jr. U.S. Patent 5,662,478.**

7.1 As regards independent **Claim 10** the *Gleichauf et al.* reference discloses a security modeling system **(Col. 2 Lines 47-50, Col. 4 Lines 20-43),** a network configuration module having network configuration data **(Col. 4 Lines 9-19 Figure 2, Col. 5 Lines 14-26),** a computer implemented method of analyzing networks based on the network configuration data where the software includes a network vulnerabilities database where the network vulnerabilities database includes, a plurality of known network vulnerabilities **(Figures 1-5, Figure 5 ITEMS 26 and 126, Col. 6 Lines 21-25, Col. 7 Lines 5-54).**

However, the *Gleichauf et al.* reference does not expressly disclose a network simulation or a mission objectives module coupled to the simulator used to determine network components that are involved in a specific attack scenario.

The *Ptacek et al.* reference discloses a network simulation for analyzing attacks against a network **(Col. 3 Lines 24-43).**

It would have been obvious, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Ptacek et al.* reference because, *(motivation to combine)* the *Ptacek et al.* reference discloses a method of simulating attacks on a network and provides a means to test the vulnerability of an proposed network configuration against different types of attacks without exposing that network to an actual attack.

However, the *Gleichauf et al.* reference does not expressly disclose a network simulation.

The *Samfate et al.* reference discloses a network simulator **(page 766).**

It would have been obvious, to one of ordinary skill in the art, at the time the invention was made, to have combined the *Network vulnerability database* of the *Gleichauf et al.* reference with the network simulator of the *Samfate et al.* reference because, by being able to exactly repeat the manner in which the network behaves as the attack takes place, software counter measures can be tested, and then retested in an environment where the same conditions can be repeated when debugging the counter measure software ***(Samfate et al. page 766).***

The *Bergmann et al.* reference discloses determining network components that are involved in a specific attack scenario **(Figures 9-14, Col. 2 Lines 6-19).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Bergmann et al.* reference because *(motivation to combine)* the *Bergmann et al.* reference discloses that it is critical that the nodes where the attack originates be located or the attack will spread **(Bergmann et al. Col. 2 Lines 6-9).**

The *Smith Jr.* reference discloses mission objectives **(Col. 4 Lines 16-25).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Smith, Jr.* reference because *(motivation to combine)* the *Smith Jr.* reference discloses a method of reducing the time required to lead a group through a creative *brain storming* process which results in more cost effective results **(Smith Jr. Col. 1 Lines 30-34).**

7.2 As regards dependent **Claim 11** the *Gleichauf et al.* reference discloses a database, including network vulnerability and exploitation data and attack data **(Figure 2 ITEM 80, Figure 3A ITEM 98, Figure 3B, 4 and 5, Col. 4 Lines 9-19, Col. 8 Lines 13-25).**

7.3 As regards dependent **Claim 13** the *Gleichauf et al.* reference does not expressly disclose a Graphical User Interface.

The *Ptacek et al.* reference discloses a Graphical User Interface **(Figure 2A, ITEM 260, Col. 4 Lines 59-67, Col. 5 Lines 1-9).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Ptacek et al.* reference because, *(motivation to combine)* a Graphical User Interface provides an easy to use method of user interaction with a computer program that does not require the user to memorize large amounts of command line interface commands to perform useful tasks.

7.4 As regards dependent **Claim 14** the *Gleichauf et al.* reference discloses goals, expectations and constraints **(Col. 1 Lines 1-67, Col. 2 Lines 1-65).**

7.5 As regards dependent **Claim 16** the *Gleichauf et al.* reference discloses a portable modeling system **(Figure 1 ITEMS 20, 22, 24 and 26).**

8. Dependent **Claims 12 and 15** are being rejected under 35 U.S.C. 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362** and in further view of "**A GSM Simulation Platform for Intrusion Detection**" by **Didier Samfat, Veronique Devernay and Christian Bonnet** *hereafter referred to as the Samfate et al. reference* and in further view of **Bergman et al. U.S. Patent 6,422,694** and in further view of **Smith, Jr. U.S. Patent 5,662,478** and in further view of **Gleichauf et al. U.S. Patent 6,282,546** *hereafter referred to as the G2 reference.*

8.1 As regards independent **Claim 10** see the rejection in paragraph 7.1 above.

8.2 As regards dependent **Claim 12** the *Gleichauf et al.* reference does not expressly disclose database tables.

The *G2* reference discloses database tables **(Figure 3B and 3C).**

It would have been obvious to combine the *Gleichauf et al.* reference with the *G2* reference because, the *Gleichauf et al.* reference specifically points the reader to the *G2* reference in **(Col. 8 Lines 12-25)** when discussing another embodiment of the invention disclosed in the *Gleichauf et al.* reference.

8.3 As regards dependent **Claim 15** the *Gleichauf et al.* reference does not expressly disclose receiving the network vulnerability, attack and exploitation data.

The *G2* reference discloses receiving updated network vulnerability, attack and exploitation data **(Figure 1 ITEMS 18 and 16).**

It would have been obvious to combine the *Gleichauf et al.* reference with the *G2* reference because, the *Gleichauf et al.* reference specifically points the reader to the *G2* reference in **(Col. 8 Lines 12-25)** when discussing another embodiment of the invention disclosed in the *Gleichauf et al.* reference.

9. Dependent **Claim 17** is rejected under 35 U.S.C. 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362** and in further view of **"A GSM Simulation Platform for Intrusion Detection"** by **Didier Samfat, Veronique Devernay and Christian Bonnet** *hereafter referred to as the Samfate et al. reference* and in further view of **Bergman'et al. U.S. Patent 6,422,694** and in further view of **Smith, Jr. U.S. Patent 5,662,478** and in further view of **Sparks, II U.S. Patent 6,352,479.**

9.1 As regards independent **Claim 10** see paragraph 7.1 above.

9.2 As regards dependent **Claim 7** the *Gleichauf et al.* reference does not expressly disclose a simulator with an attacker and a defender user interface.

The *Sparks II* reference discloses an attacker and a defender user interface **(Figure 3).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Sparks II* reference because, *(motivation to combine)* by supporting multiple players using a network and graphical user interfaces, complex and real-time interaction between an attacker and a defender can be achived over great distances using a network, like the internet, where two people do not have to be in the same geographic location to play against each other in a simulation or a game ***(Sparks II, Col. 1 Lines 50-65*).**

10. Dependent **Claim 20** is rejected under 35 U.S.C 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362** and in further view of "**A GSM Simulation Platform for Intrusion Detection**" by **Didier Samfat, Veronique Devernay and Christian Bonnet** *hereafter referred to as the Samfate et al. reference* and in further view of **Ballard et al. U.S. Patent 4,937,825.**

10.1 As regards independent **Claim 18** see paragraph 3.1 above.

10.2 As regards dependent **Claim 20** the *Gleichauf et al.* reference does not expressly disclose network configuration files.

The *Ballard et al.* reference discloses network configuration files **(Col. 2 Lines 10-53).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Ballard et al.* reference because *(motivation to combine)* the *Ballard et al.* reference discloses a method and apparatus for isolating and diagnosing problems in a data communications network **(Col. 1 Lines 58-68),** an artisan would be drawn to this teaching because it shows how to monitor and document the configuration of a data network which saves time and effort when trying to fix a problem.

11. Dependent **Claims 21, 22, 23 and 26** are rejected under 35 U.S.C 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362** and in further view of "**A GSM Simulation Platform for Intrusion Detection"** by **Didier Samfat, Veronique Devernay and Christian Bonnet** *hereafter referred to as the Samfate et al. reference* and in further view of **"HACKER, The Computer Crime Card Game", by Steve Jackson** hereafter referred to as the *Jackson* reference.

11.1 As regards independent **Claim 18,** see paragraph 3.1 above.

11.2 As regards dependent **Claim 21,** the *Gleichauf et al.* reference does not expressly disclose mission objectives.

The *Jackson* reference discloses mission objectives **(Page 7 "WINNING THE GAME").**

It would have been obvious, to one of ordinary skill in the art, to have modified the *Gleichauf et al.* reference with the *Jackson* reference because, *(motivation to combine)* modeling a computer network and pretending to hack into that network are activities that people like to do, as shown in the *Jackson* reference **(Page 1, INTRODUCTION).**

11.3 As regards dependent **Claim 22,** the *Gleichauf et al.* reference does not expressly disclose a Graphical User Interface.

The *Ptacek et al.* reference discloses a Graphical User Interface **(Figure 2A, ITEM 260, Col. 4 Lines 59-67, Col. 5 Lines 1-9).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Ptacek et al.* reference because, *(motivation to combine)* a Graphical User Interface provides an easy to use method of user interaction with a computer program that does not require the user to memorize large amounts of command line interface commands to perform useful tasks.

11.4 As regards dependent **Claim 23**, the *Gleichauf et al.* reference does not expressly disclose dynamically interacting with an attacker.

The *Jackson* reference discloses interacting with an attacker **(Pages 2-7).**

It would have been obvious, to one of ordinary skill in the art, to have modified the *Gleichauf et al.* reference with the *Jackson* reference because, *(motivation to combine)* modeling a computer network and pretending to hack into that network are activities that people like to do, as shown in the *Jackson* reference **(Page 1, INTRODUCTION).**

11.5 As regards dependent **Claim 26** the *Gleichauf et al.* reference does not expressly disclose a score.

The *Jackson* reference discloses a score **(Page 7, WINNING THE GAME).**

It would have been obvious, to one of ordinary skill in the art, to have modified the *Gleichauf et al.* reference with the *Jackson* reference because, *(motivation to combine)* modeling a computer network and pretending to hack into that network are activities that people like to do, as shown in the *Jackson* reference **(Page 1, INTRODUCTION).**

12. Dependent **Claims 23, 24 and 25** are rejected under 35 U.S.C 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362** and in further view of **"A GSM Simulation Platform for Intrusion Detection"** by **Didier Samfat, Veronique Devernay and Christian Bonnet** *hereafter referred to as the Samfate et al. reference* and in further view of **"HACKER, The Computer Crime Card Game", by Steve Jackson** herafter referred to as the *Jackson* reference and in further view of **Kurtzberg et al. U.S. Patent 5,961,644**.

12.1 As regards independent **Claim 18,** see paragraph 3.1 above.

12.2 As regards dependent **Claim 21,** see paragraph 11.2 above.

12.3 As regards dependent **Claim 22,** see paragraph 11.3 above.

12.4 As regards dependent **Claim 23,** the *Gleichauf et al.* reference does not expressly disclose dynamically interacting with an attacker.

The *Kurtzberg et al.* reference discloses dynamically interacting with an attacker **(Figure 6, Col. 3 Lines 20-67, Col. 4 Lines 1-15).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Kurtzberg et al.* reference because, *(motivation to combine)* attack simulations allow for testing of network security mechanisms and training of security systems administrators **(Kurtzberg et al. Col. 1 Lines 5-67).**

12.5 As regards dependent **Claims 24 and 25** the *Gleichauf et al.* reference does not expressly disclose interacting in real time with a security modeling system.

The *Kurtzberg et al.* reference discloses interacting in real time with a security modeling system **(Figure 6, Col. 3 Lines 20-67, Col. 4 Lines 1-15).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Kurtzberg et al.* reference because, *(motivation to combine)* attack simulations allow for testing of network security mechanisms and training of security systems administrators **(Kurtzberg et al. Col. 1 Lines 5-67).**

13. Dependent **Claim 27** is rejected under 35 U.S.C 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362** and in further view of "**A GSM Simulation Platform for Intrusion Detection**" by **Didier Samfat, Veronique Devernay and Christian Bonnet** *hereafter referred to as the Samfate et al. reference* and in further view of **"HACKER, The Computer Crime Card Game", by Steve Jackson** hereafter referred to as the *Jackson* reference and in further view of **Gleichauf et al. U.S. Patent 6,282,546** *hereafter referred to as the G2 reference.*

13.1 As regards independent **Claim 18,** see paragraph 3.1 above.

13.2 As regards dependent **Claim 21,** see paragraph 11.2 above.

13.3 As regards dependent **Claim 27** the *Gleichauf et al.* reference does not expressly disclose updating the vulnerabilities data base.

The *G2* reference discloses receiving updated network vulnerability, attack and exploitation data **(Figure 1 ITEMS 18 and 16).**

It would have been obvious to combine the *Gleichauf et al.* reference with the *G2* reference because, the *Gleichauf et al.* reference specifically points the reader to the *G2* reference in **(Col. 8 Lines 12-25)** when discussing another embodiment of the invention disclosed in the *Gleichauf et al.* reference.

14. Independent **Claim 28** and dependent **Claims 29 and 30** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **"Simulated Attack for Real Network Security" by Johna Till Johnson**, *hereafter referred to as the Johnson* reference, and in further view of **"A GSM Simulation Platform for Intrusion Detection"** by **Didier Samfat, Veronique Devernay and Christian Bonnet** *hereafter referred to as the Samfate et al. reference* and in further view of **Kurtzberg et al. U.S. Patent 5,961,644** and in further view of **"HACKER, The Computer Crime Card Game", by Steve Jackson** hereafter referred to as the *Jackson* reference.

14.1 As regards independent **Claim 28** the *Gleichauf et al.* reference discloses a method of opposing network attackers **(Figure 1, ITEMS 40, 42, 44 and 46, Figure 2 ITEM 80, Col. 1 Lines 10-21)**, receiving a network configuration comprising hardware and software component information **(Figure 2,** *note device type [hardware] and services [software],* **Col. 4 Lines 20-42, Col. 5 Lines 14-26)**, determining results as a function of network configuration, and stored vulnerability data for the described computer hardware and software components **(Figure 1 Item 26, Figures 3A-5, Col. 8 Lines 12-25).**

However, the *Gleichauf et al.* reference does not expressly disclose; simulated network attacks, mission objectives, receiving commands from a network attacker and responding to the attack.

The *Johnson* reference discloses a simulated network attack **(Pages 31-32).**

It would have been obvious, to one of ordinary skill in the at, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Johnson* reference because, *(motivation to combine)* the *Johnson* reference discloses a good method for preventing unauthorized access to a data network **(Johnson page 31-32).**

However, the *Gleichauf et al.* reference does not expressly disclose a network simulation.

The *Samfate et al.* reference discloses a network simulator **(page 766).**

It would have been obvious, to one of ordinary skill in the art, at the time the invention was made, to have combined the *Network vulnerability database* of the *Gleichauf et al.* reference with the network simulator of the *Samfate et al.* reference because, by being able to exactly repeat the manner in which the network behaves as the attack takes place, software counter measures can be tested, and then retested in an environment where the same conditions can be repeated when debugging the counter measure software ***(Samfate et al. page 766*).**

The *Kurtzberg et al.* reference discloses receiving commands from a network attacker **(Figure 6, Col. 3Lines 20-28),** and responding to the attack **(Col. 3 Lines 40-67, Col. 4 Lines 1-15).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Kurtzberg et al.* reference because, *(motivation to combine)* attack simulations allow for testing of network security mechanisms and training of security systems administrators **(Kurtzberg et al. Col. 1 Lines 5-67).**

The *Jackson* reference discloses mission objectives **(Page 7 WINNING THE GAME).**

It would have been obvious, to one of ordinary skill in the art, to have modified the *Gleichauf et al.* reference with the *Jackson* reference because, *(motivation to combine)* modeling a computer network and pretending to hack into that network are activities that people like to do, as shown in the *Jackson* reference **(Page 1, INTRODUCTION).**

14.2 As regards dependent **Claim 29** the *Gleichauf et al.* reference does not expressly disclose defender commands.

The *Kurtzberg et al.* reference discloses defender commands **(Figure 6,** *YES result***).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Kurtzberg et al.* reference because, *(motivation to combine)* attack simulations allow for testing of network security mechanisms and training of security systems administrators **(Kurtzberg et al. Col. 1 Lines 5-67).**

14.3 As regards dependent **Claim 30** the *Gleichauf et al.* reference does not expressly disclose receiving critical resource information.

The *Johnson* reference discloses critical resource information **(Page 31, specified set of IP addresses).**

It would have been obvious, to one of ordinary skill in the at, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Johnson* reference because, *(motivation* *to combine)* the *Johnson* reference discloses a good method for preventing unauthorized access to a data network **(Johnson page 31-32).**

15. Dependent **Claims 31-33** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **"Simulated Attack for Real Network Security" by Johna Till Johnson,** *hereafter referred to as the Johnson* reference, and in further view of "**A GSM Simulation Platform for Intrusion Detection"** by **Didier Samfat, Veronique Devernay and Christian Bonnet** *hereafter referred to as the Samfate et al. reference* and in further view of **Kurtzberg et al. U.S. Patent 5,961,644** and in further view of **"HACKER, The Computer Crime Card Game", by Steve Jackson** hereafter referred to as the *Jackson* reference and in further view of **Porras et al. U.S. Patent 6,321,338.**

15.1 As regards independent **Claim 28** see paragraph 14.1 above.

15.2 As regards dependent **Claim 31** the *Gleichauf et al.* reference does not expressly disclose a graphical user interface.

The *Porras et al.* reference discloses a GUI **(Figure 5 Items 54, 50 and 58, Col. 14 Lines 50-58).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Porras et al.* reference because *(motivation to combine)* the ability to do statistical analysis on packet usage allows for detection of subtle network intrusions not easily detectable using non-statistical means **(Porras et al. Col. 1 Lines 42-54).**

15.3 As regards dependent **Claim 32** the *Gleichauf et al.* reference does not expressly discloses a security score.

The *Porras et al.* reference discloses a security score **(Col. 11 Lines 57-67, Col. 12 Lines 1-6).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Porras et al.* reference because *(motivation to combine)* the ability to do statistical analysis on packet usage allows for detection of subtle network intrusions not easily detectable using non-statistical means **(Porras et al. Col. 1 Lines 42-54).**

15.4 As regards dependent **Claim 33** the *Gleichauf et al.* reference does not expressly disclose receiving attack commands that change services or nodes and that exploit vulnerabilities.

The *Kurtzberg et al.* reference discloses receiving attack commands that change services or nodes and that exploit vulnerabilities **(Figure 6, Col. 3 Lines 40-67, Col. 4 Lines 1-15).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Kurtzberg et al.* reference because, *(motivation to combine)* attack simulations allow for testing of network security mechanisms and training of security systems administrators **(Kurtzberg et al. Col. 1 Lines 5-67).**

16. Independent **Claims 34 and 40** and dependent **Claims 35-38, 41 and 42** are being rejected under 35 U.S.C. 103(a) as being unpatentable over **"Simulated Attack for Real**

Network Security" by Johna Till Johnson, *hereafter referred to as the Johnson* reference in view of **Porras et al. U.S. Patent 6,321,338** and in further view of "**A GSM Simulation Platform for Intrusion Detection**" by **Didier Samfat, Veronique Devernay and Christian Bonnet** *hereafter referred to as the Samfate et al. reference* and in further view of **Gleichauf et al. U.S. Patent 6,282,546.**

16.1 As regards independent **Claims 34 and 40** the *Johnson* reference discloses a security modeling system for simulating networks and to determine network components that are involved in a specific attack scenario including configuration data **(Pages 31-32).**

However, the *Johnson* reference does not expressly disclose, a plurality of data bases including mission objective tables, vulnerability tables and network configuration tables as well as a graphical user interface.

The *Gleichauf et al.* reference discloses a plurality of data bases including mission objective tables, vulnerability tables and network configuration tables **(Figure 1, Figures 3A, 3B, 3C, 3D,)** and configuration tables **(TABLE 1 Col. 5 Lines 45-53).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Johnson* reference with the *Gleichauf et al.* reference because, *(motivation to combine)* organizing data into tables is well known in the art and the *Gleichauf et al.* reference discloses good methods of organizing data related to Network Security Vulnerability testing in such a manner that allows for flexibility and efficiency ***(Gleichauf et al.*** **Col. 1 Lines 58-63).**

The *Porras et al.* reference discloses the use of a Graphical User Interface **(Col. 14 Lines 51-58).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Johnson* reference with the *Porras et al.* reference because, *(motivation to combine)* a Graphical User Interface provides an easy to use method of user interaction with a computer program that does not require the user to memorize large amounts of command line interface commands to perform useful tasks.

However, the *Johnson* reference does not expressly disclose a network simulation.

The *Samfate et al.* reference discloses a network simulator **(page 766).**

It would have been obvious, to one of ordinary skill in the art, at the time the invention was made, to have combined the *Johnson* reference with the network simulator of the *Samfate et al.* reference because, by being able to exactly repeat the manner in which the network behaves as the attack takes place, software counter measures can be tested, and then retested in an environment where the same conditions can be repeated when debugging the counter measure software ***(Samfate et al. page 766).***

16.2 As regards dependent **Claims 35 and 41** the *Johnson* reference does not expressly disclose mission tables or files.

The *Gleichauf et al.* reference discloses a plurality of data bases including mission objective tables, vulnerability tables and network configuration tables **(Figure 1, Figures 3A, 3B, 3C, 3D,)** and configuration tables **(TABLE 1 Col. 5 Lines 45-53).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Johnson* reference with the *Gleichauf et al.* reference because, *(motivation to combine)* organizing data into tables is well known in the art and the *Gleichauf et al.* reference discloses good methods of organizing data related to Network Security

Vulnerability testing in such a manner that allows for flexibility and efficiency ***(Gleichauf et al.* Col. 1 Lines 58-63).**

16.3 As regards dependent **Claim 36** the *Johnson* reference does not expressly disclose service tables.

The *Gleichauf et al.* reference discloses a service table **(Figure 5B).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Johnson* reference with the *Gleichauf et al.* reference because *(motivation to combine)* the ability to catalog services in a database is useful because there can be a record of which services are authorized and the data base can be used as an audit tool to determine what has happened after an attack ***(Gleichauf et al. Col. 2 Lines 36-40*).**

16.4 As regards dependent **Claim 37** the *Johnson* reference does not expressly disclose configuration tables, defense tables, node tables, routing tables and password tables.

The *Gleichauf et al.* reference discloses configuration tables, defense tables, node tables, routing tables and password tables **(Col. 5 Lines 8-36).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Johnson* reference with the *Gleichauf et al.* reference because *(motivation to combine)* the ability to catalog services in a database is useful because there can be a record of which services are authorized and the data base can be used as an audit tool to determine what has happened after an attack ***(Gleichauf et al. Col. 2 Lines 36-40*).**

16.5 As regards dependent **Claim 38** the *Johnson* reference does not expressly disclose transmitting real-time network information

The *Porras et al.* reference discloses real-time monitoring **(Col. 3 Lines 42-54).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Johnson* reference with the *Porras et al.* reference because, *(motivation to combine)* to be able to monitor events in real-time the amount of damage from a network intrusion can be minimized.

16.6 As regards dependent **Claim 42** the *Johnson* reference does not expressly disclose determining which network components are involved in a specific network attack.

The *Gleichauf et al.* reference discloses determining which network components are involved in a specific network attack **(Figures 6A, 6B, Col. 7 Lines 29-42).**

It would have been obvious, to one of ordinary skill in the art, at the time of the invention, to have modified the *Johnson* reference with the *Gleichauf et al.* reference because *(motivation to combine)* different devices on a computer network have different vulnerabilities and it is useful to have a central database to distinguish which device is being attacked and what vulnerabilities are present on that specific platform ***(Gleichauf et al. Col. 7 Lines 29-42*).**

17. Independent **Claim 9** and dependent **Claim 39** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Gleichauf et al. U.S. Patent 6,324,656** in view of **Ptacek et al. U.S. Patent 6,343,362** and in further view of "**A GSM Simulation Platform for Intrusion Detection**" by **Didier Samfat, Veronique Devernay and Christian Bonnet** *hereafter referred to as the Samfate et al. reference* and in further view of **"HACKER, The Computer Crime Card Game", by Steve Jackson** hereafter referred to as the *Jackson* reference.

17.1 As regards independent **Claim 9** the *Gleichauf et al.* reference discloses a network configuration module **(Col. 4 Lines 9-19 Figure 2, Col. 5 Lines 14-26),** a computer implemented method of analyzing networks based on the network configuration data where the software includes a network vulnerabilities database where the network vulnerabilities database includes, a plurality of known network vulnerabilities where each network vulnerability includes a service to which it applies, defense conditions that might close the vulnerability, and resource and state conditions needed to exercise the vulnerability, **(Figures 1-5, Figure 5 ITEMS 26 and 126, Col. 6 Lines 21-25, Col. 7 Lines 5-54).**

However, the *Gleichauf et al.* reference does not expressly disclose a network simulation or a computer game.

The *Ptacek et al.* reference discloses a network simulation for analyzing attacks against a network **(Col. 3 Lines 24-43).**

It would have been obvious, at the time of the invention, to have modified the *Gleichauf et al.* reference with the *Ptacek et al.* reference because, *(motivation to combine)* the *Ptacek et al.* reference discloses a method of simulating attacks on a network and provides a means to test the vulnerability of an proposed network configuration against different types of attacks without exposing that network to an actual attack.

The *Jackson* reference discloses a game **(Pages 1-8).**

It would have been obvious, to one of ordinary skill in the art, to have modified the *Gleichauf et al.* reference with the *Jackson* reference because, *(motivation to combine)* modeling a computer network and pretending to hack into that network are activities that people like to do, as shown in the *Jackson* reference **(Page 1, INTRODUCTION).**

The *Gleichauf et al.* reference does not expressly disclose a network simulation.

The *Samfate et al.* reference discloses a network simulator **(page 766).**

It would have been obvious, to one of ordinary skill in the art, at the time the invention was made, to have combined the *Network vulnerability database* of the *Gleichauf et al.* reference with the network simulator of the *Samfate et al.* reference because, by being able to exactly repeat the manner in which the network behaves as the attack takes place, software counter measures can be tested, and then retested in an environment where the same conditions can be repeated when debugging the counter measure software ***(Samfate et al. page 766*****).**

17.2 As regards dependent **Claim 39** the *Gleichauf et al.* reference does not expressly disclose mission objectives, critical resource information and specific attack scenario information.

The *Jackson* reference discloses mission objectives, critical resource information and specific attack scenario information, **(Pages 1-8).**

It would have been obvious, to one of ordinary skill in the art, to have modified the *Gleichauf et al.* reference with the *Jackson* reference because, *(motivation to combine)* modeling a computer network and pretending to hack into that network are activities that people like to do, as shown in the *Jackson* reference **(Page 1, INTRODUCTION).**

18. **Claims 1-8, 10-15, 18-22, 25-27, 28-33, 34-37, 40-42** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Kondo et al. U.S. Patent 5,684,957** in view of **Shostack et al. U.S. Patent 6,298,445.**

18.1 As regards independent **Claims 1, 10, 18, 28, 34 and 40** the *Kondo et al.* reference discloses a network simulation and model for use in intrusion detection of a computer network **(Figure 12, 20, 36, 38 and 39, Col. 3 lines 16-27, Col. 4 lines 55-59, Col. 5 lines 1-67,**

Col. 6 lines 1-67), including using real-time accurate data from an actual network **(Col. 13 Lines 50-63),** and using databases of network exploits and countermeasures to protect and *fix* the network in real-time **(Col. 5 lines 47-39)** and a objective module **(Col. 7 lines 22-35).**

However, the *Kondo et al.* reference does not expressly disclose a specific database of network vulnerabilities.

The *Shostack et al.* reference discloses a database of security vulnerabilities **(Figure 6 item 92).**

It would have been obvious, to one of ordinary skill in the network security art, to update the network security methods of the *Kondo et al.* database with the database of security vulnerability in the *Shostack et al.* reference, at the time the invention was made because, *Whenever an unauthorized user breaches network security and is allowed free access to the system, the damage that might result is unpredictable... the system administrator is required to remain constantly vigilant as to new attacks being used by hackers, and then use that information to protect the network, clients and servers from the newly found vulnerability.* **(Shostack et al. Col. 2 lines 18-29).** Thus, an artisan of ordinary skill would want to *update* the *Kondo et al.* reference with the methods of the *Shostack et al.* reference so that newer threats to the network could be effectively defended against.

18.2 As regards dependent **Claims 2-8, 11-17, 19-22, 29-33, 35-37, 41 and 42**

The *Kondo et al.* reference does discloses the functional equivalent of a network discovery tool **(Col. 3 lines 16-27)** and a display means **(Col. 6 lines 42-50).**

However, the *Kondo et al.* reference does not expressly disclose a GUI and a vulnerability database.

The *Shostack et al.* reference discloses a GUI **(Figure 6)** and a vulnerability database **(Figure 6 item 92).**

As regards the motivation to combine the two references please see section **18.1** of this Office Action.

Conclusion

19. **Claims 1-42** are rejected. Prosecution is reopened. This action is **Non-Final.**

19.1 Any inquiry concerning this communication or earlier communications from the examiner should be directed to Dwin M Craig whose telephone number is (571) 272-3710. The examiner can normally be reached on 10:00 - 6:00 M-F.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kevin Teska can be reached on (571)272-3716. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DMC

KEVIN J. TESKA
SUPERVISORY
PATENT EXAMINER